ABSTRACT OF THE DISCLOSURE

A technique for detecting Trojans and worms within packed computer files uses fingerprint data derived from the unpacked resource data associated with the packed computer files. The number of entries, the position within the resource data and size of the resource that is the largest resource specified, a timestamp value of compilation and a checksum value derived from the whole of the resource data may be included within a fingerprint value as characteristic of a particular set of resource data. A library of such fingerprint values may be generated for known Trojans and worms, or other programs it is wished to detect, and then a suspect file compared against this library of fingerprints.

[Figure 6]